Cybersecurity Audit

Part 2 – Management of IT Auditing

TTÜ 2008

Foundation of IS auditing

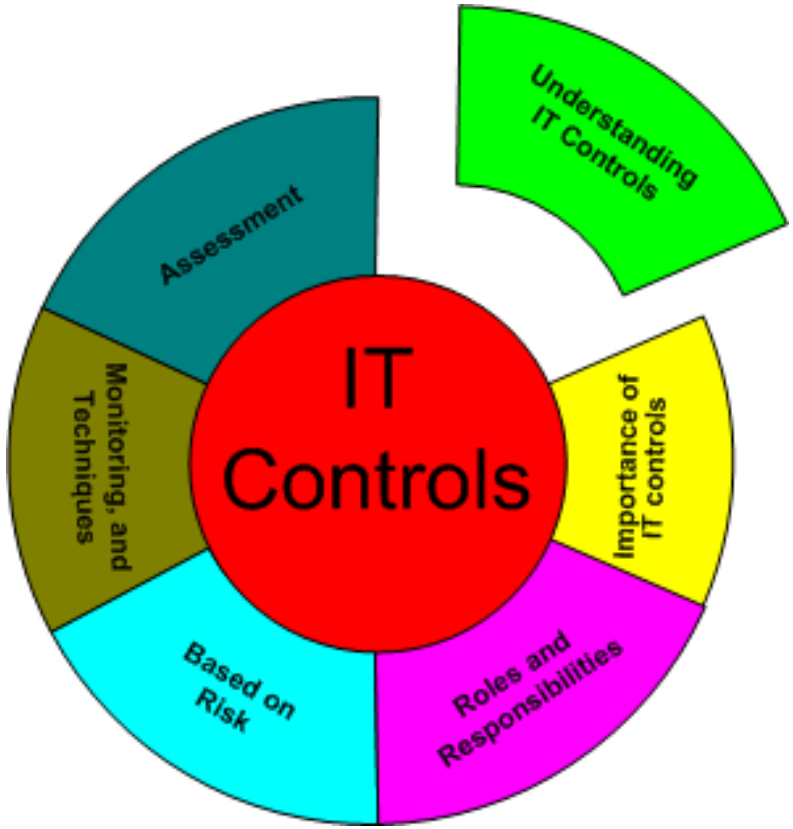
Agenda

- IT Controls
- Change and Patch Management Controls
- Continuous Auditing
- Management of IT Auditing
- Managing and Auditing IT Vulnerabilities
- IT Outsourcing
- Auditing Application Controls
- Very Short Summary

IT Controls

Understanding IT Controls

- IT control is a process that provide assurance for information and information services, and help to mitigate risks associated with use of technology.
- Two components
  - Automation of business controls
  - Control of IT



Effective Controls

- Control is “effective” to the extent that it provides reasonable assurance that the organization will achieve its objectives reliably.

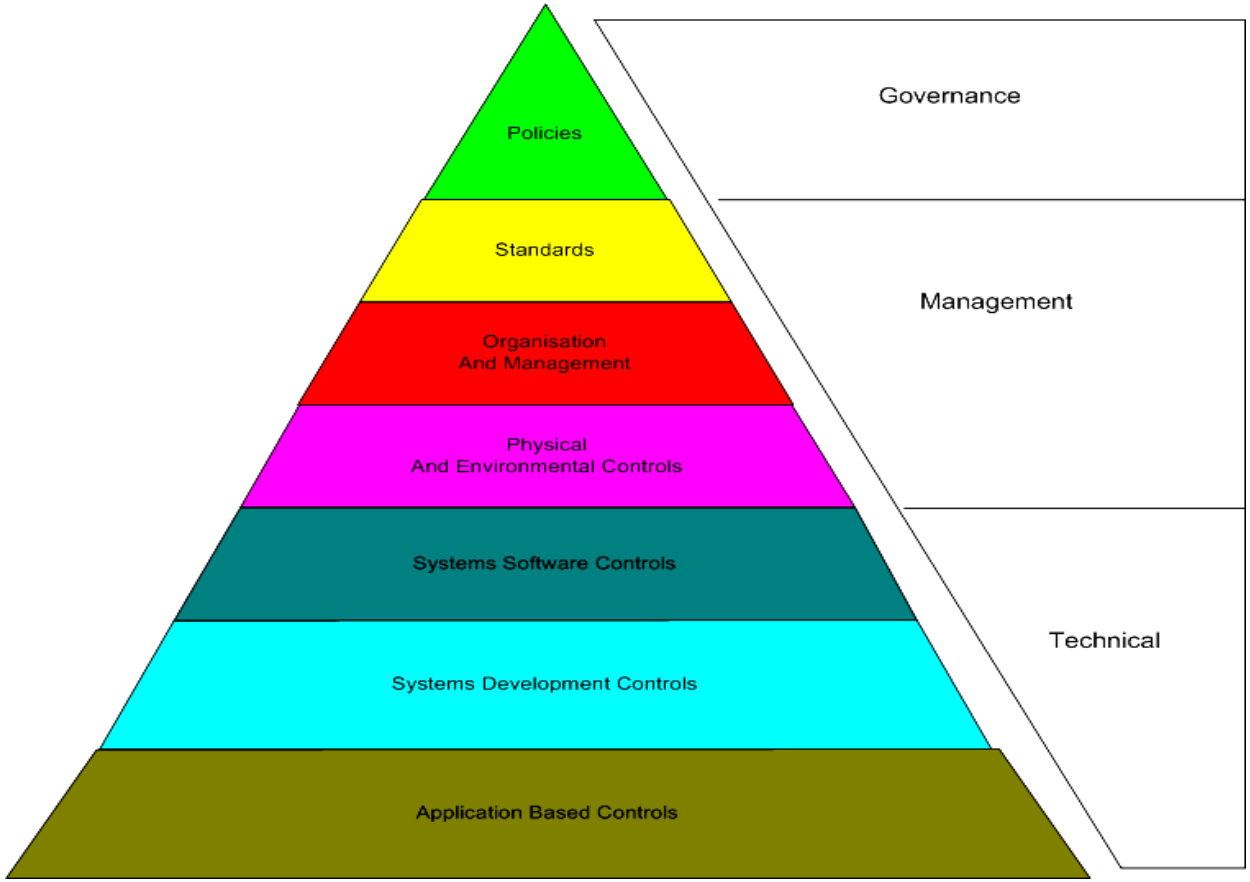
Control Risk

- Control risk measures the likelihood that the control processes established to limit or manage inherent risk are ineffective.
- In order to ensure that audit evaluates the controls properly, the auditor must understand how to measure which controls are effective.
- This will involve identifying those controls that provide the greatest degree of assurance to minimize risks within the business.
- Control effectiveness is strongly impacted by the quality of work and control supervision.

Control Risk

- Controls in business operations provide the major line of defense against inherent risk.
- In general, the auditor may assume that stronger controls reduce the amount of risk;
  - however, at some point the cost of control may become prohibitive (in terms of both monetary and staff resources as well as customer satisfaction).

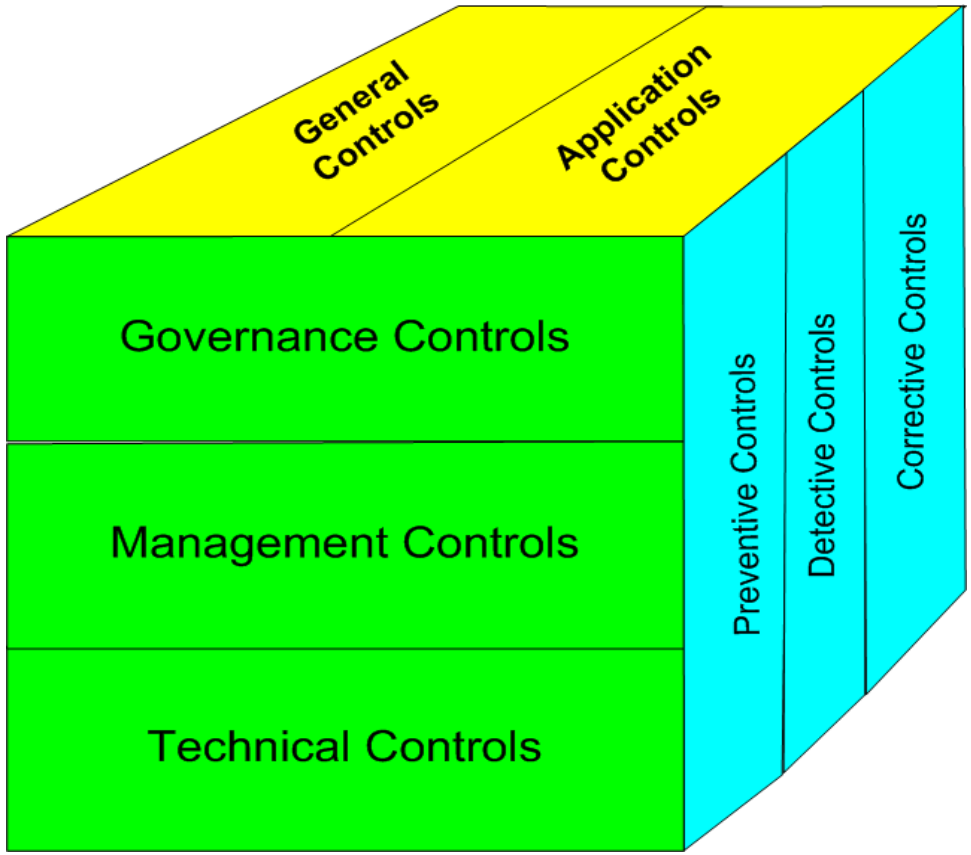
Understanding IT Controls

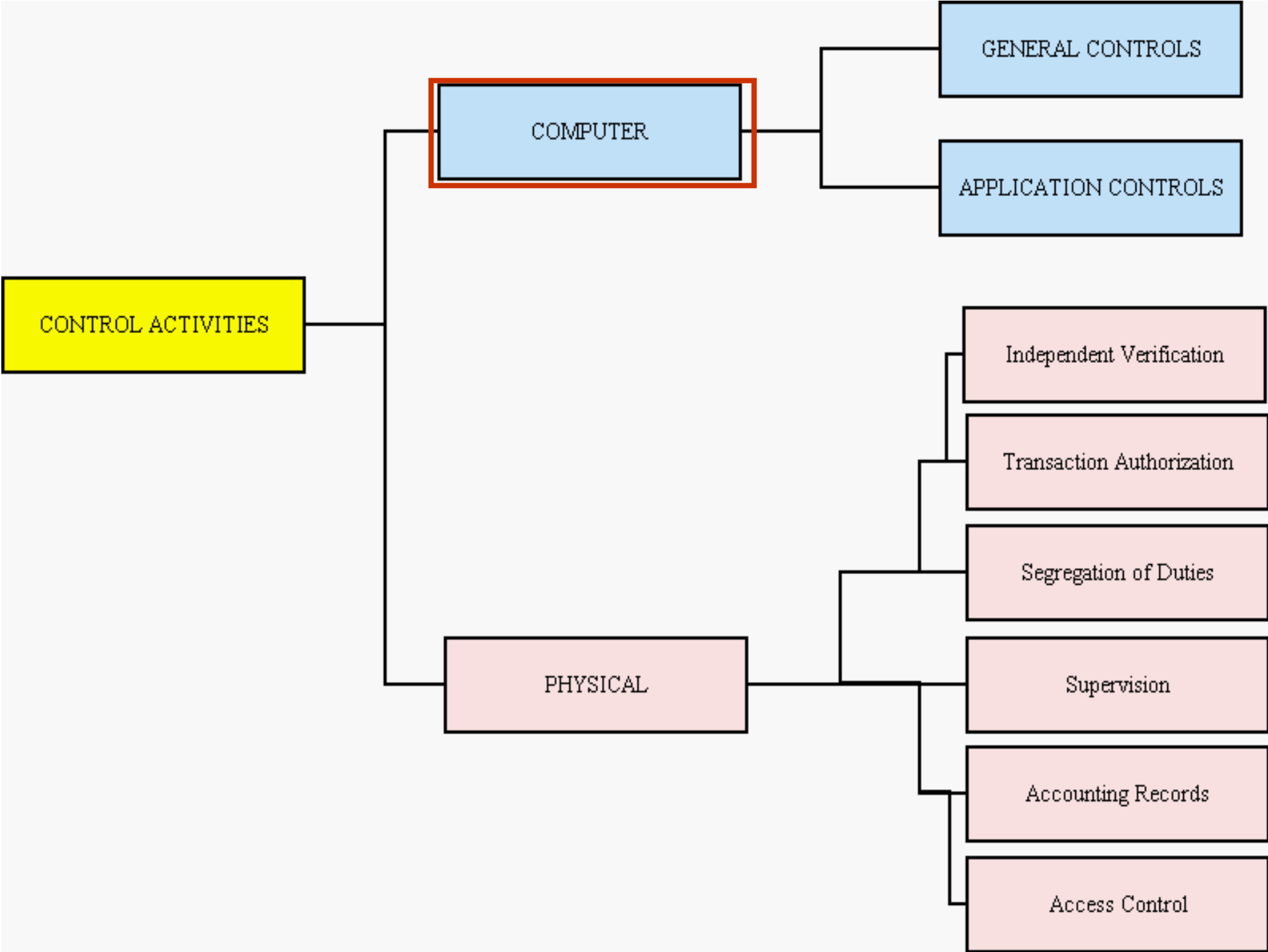


- A top-down approach used when considering controls to implement and determining areas on which to focus.

Understanding IT Controls

- Classification
  - Computer Controls
  - Physical Controls
- *Computer Controls:* Classification
  - General Controls
  - Application Controls
- Classification
  - Preventive
  - Detective
  - Corrective
- Classification
  - Governance controls
  - Management controls
  - Technical controls




CONTROL ACTIVITIES
COMPUTER
GENERAL CONTROLS
APPLICATION CONTROLS
PHYSICAL
Independent Verification
Transaction Authorization
Segregation of Duties
Supervision
Accounting Records
Access Control

General controls

- **General controls** (also known as infrastructure controls) apply to
  - all systems components,
  - processes, and
  - data for a given organization or systems environment.
- General controls include, but are not limited to:
  - information security policy,
  - administration,
  - access, and authentication;
  - backup,
  - recovery, and
  - business continuity.

Application controls

- **Application controls** pertain to the scope of individual business processes or application systems.
- They include such controls as
  - data edits,
  - transaction logging, and
  - error reporting.
- The function of a control is highly relevant to the assessment of its design and effectiveness.

Preventive controls

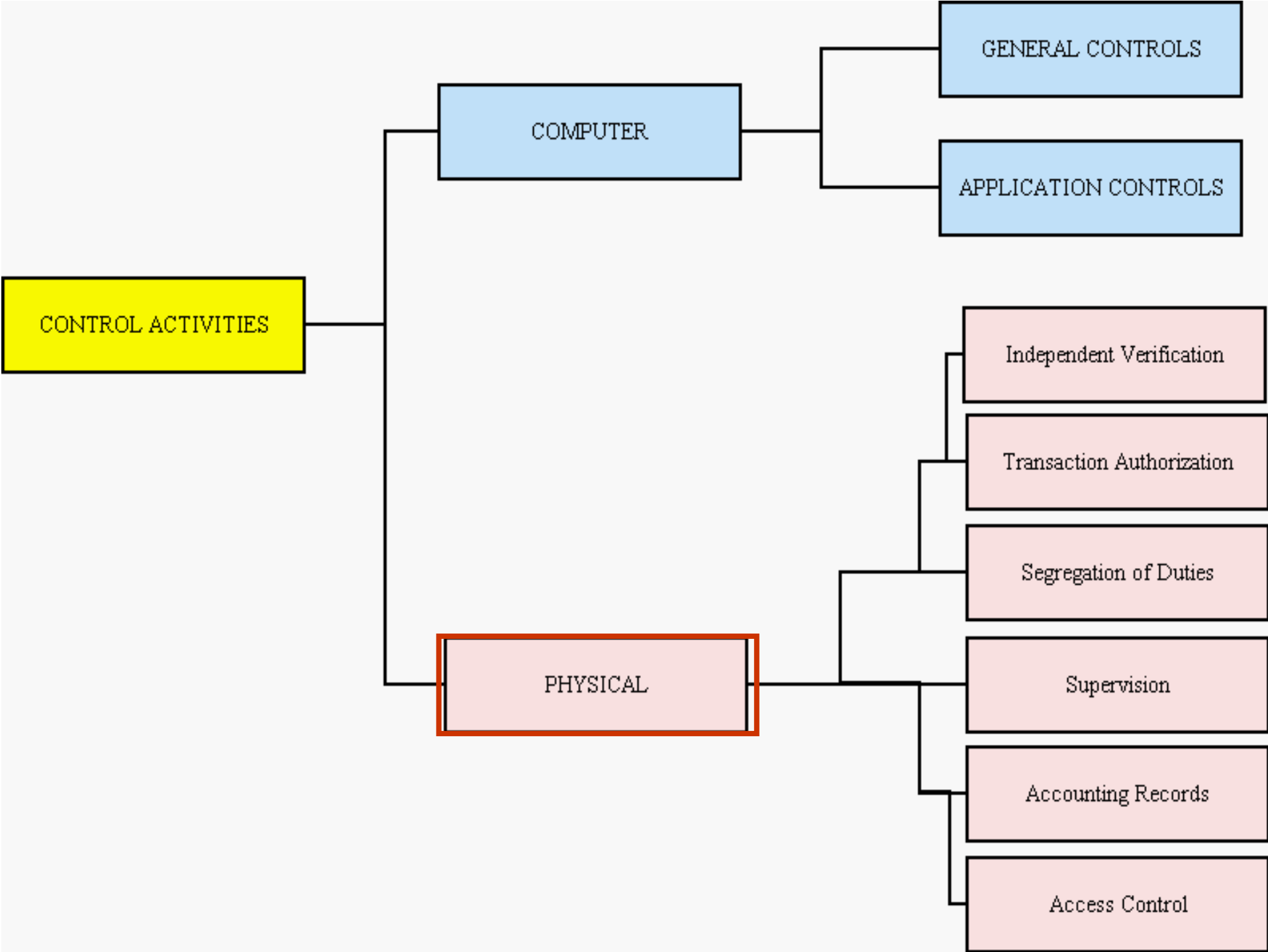
- **Preventive controls** prevent
  - errors,
  - omissions, or
  - security incidents from occurring.
  - Examples include
    - antivirus software,
    - firewalls, and
    - intrusion prevention systems.

Detective controls

- **Detective controls** detect errors or incidents that elude preventive controls.
- For example, a detective control may
  - identify account numbers of inactive accounts or
  - accounts that have been flagged for monitoring of suspicious activities.

Corrective controls

- **Corrective controls** correct
  - errors,
  - omissions, or
  - incidents once they have been detected.
- They vary from
  - simple correction of data-entry errors, to
  - recovery from incidents, or disasters.

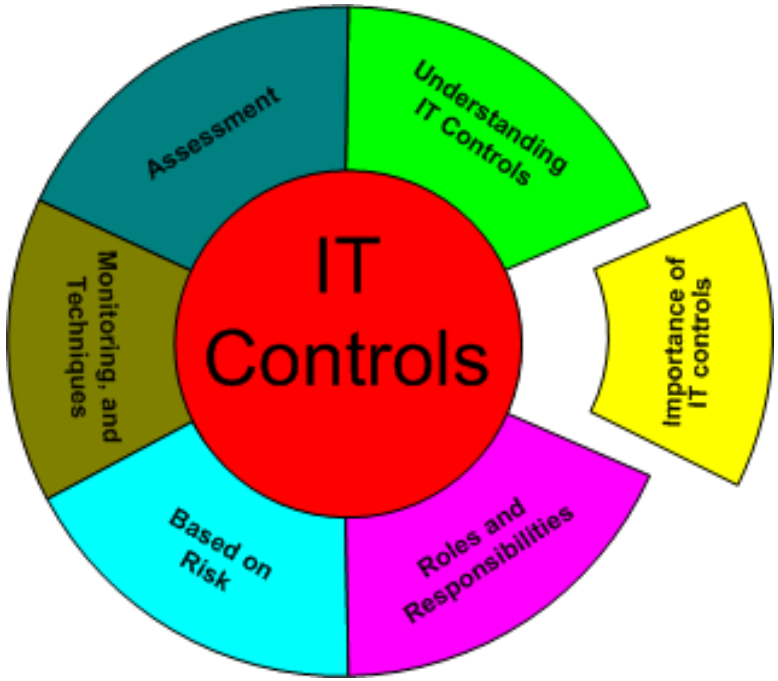

CONTROL ACTIVITIES
COMPUTER
GENERAL CONTROLS
APPLICATION CONTROLS
PHYSICAL
Independent Verification
Transaction Authorization
Segregation of Duties
Supervision
Accounting Records
Access Control

- Physical Controls (1-3)
  - Transaction authorization
    - Example:
      - Sales only to authorized customer
      - Sales only if available credit limit
  - Segregation of duties
    - Example of incompatible duties:
      - Authorization vs. processing
  - Supervision
    - Serves as compensating control when lack of segregation of duties exists by necessity

- Physical Controls (4-6)
  - Accounting records (audit trails)
  - Access controls
    - Direct (the assets)
    - Indirect (documents that control the assets)
  - Independent verification
    - Management can assess:
      - The performance of individuals
      - The integrity of the data in the records

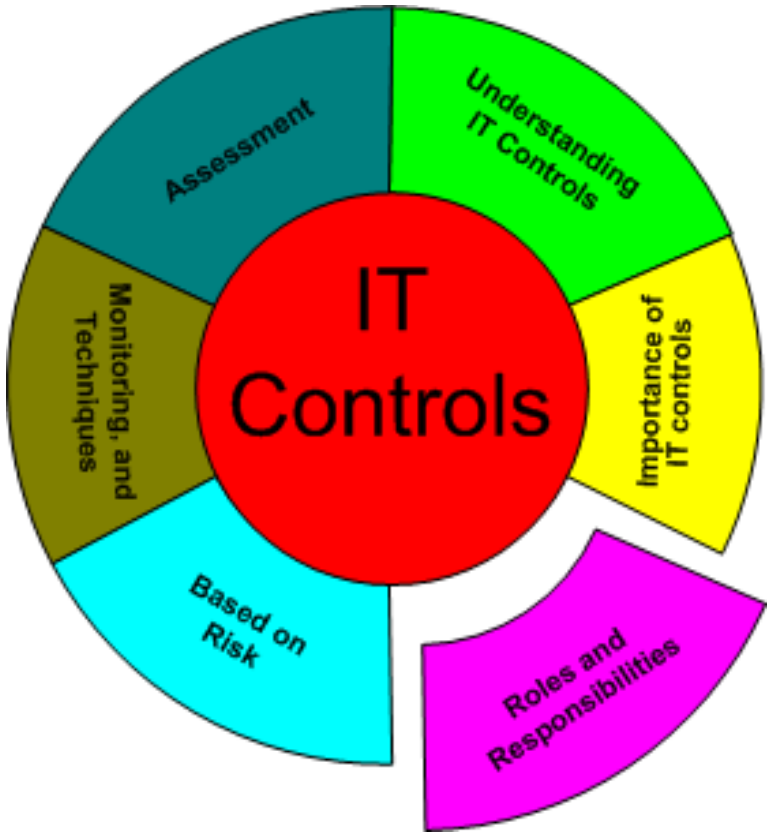
Importance of IT Controls

- Needs for IT controls, such as
  - controlling cost
  - remaining competitive
  - protecting of information assets
  - complying with laws and regulation
- Implementing effective IT control will improve
  - efficiency,
  - reliability,
  - flexibility and
  - availability of assurance evidence



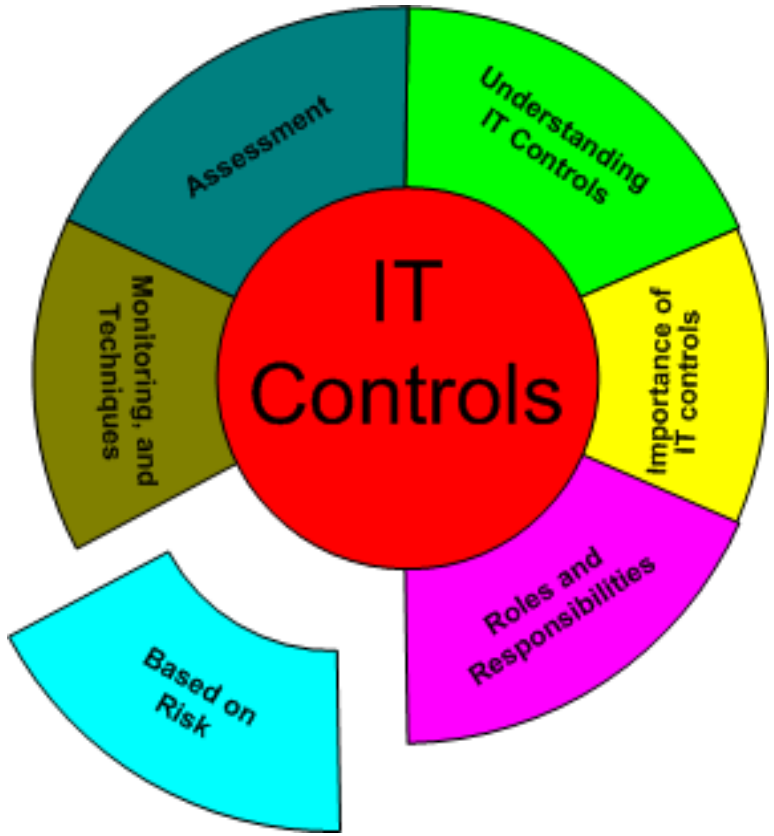
Roles and Responsibilities

- **Board of Directors** /Governing Body
- **Management** – define, approve, implement IT controls or understand the use of IT controls
- **Audit Committee** - take IT controls as strong elements in oversight of financial issues, internal control assessment, risk management, and ethics.
- **Auditor**
  - Internal Auditors - assurance
  - External Auditors – periodical auditing



Based On Risk

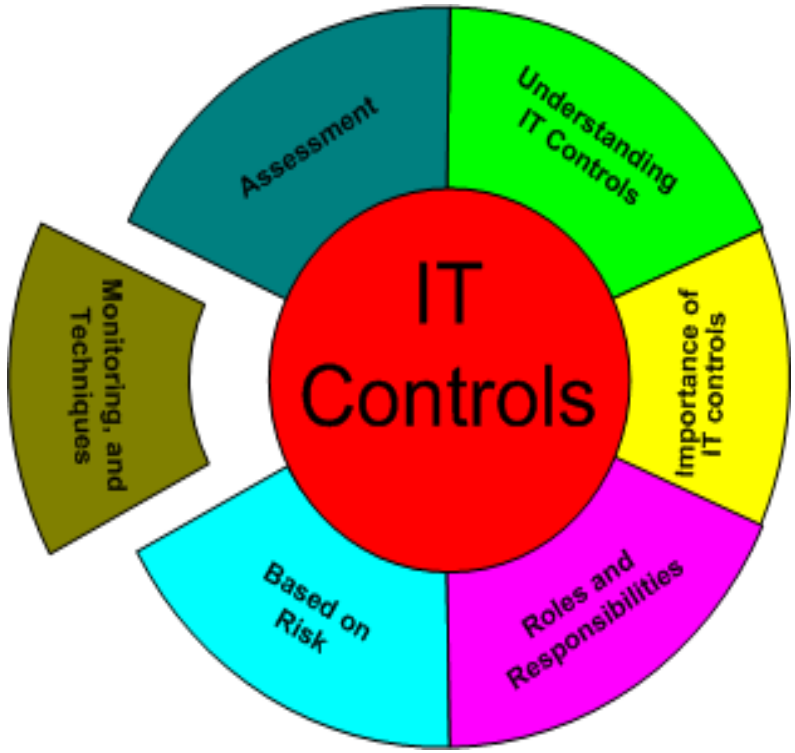
- Analyzing Risk
  - Identify risks
  - Consider risk in determining the adequacy of IT controls
  - Define risk mitigation strategy
    - accept/eliminate/share/control/ mitigate
  - Consider Baseline IT controls



IT controls are selected and implemented on the basis of the risks they are designed to manage.

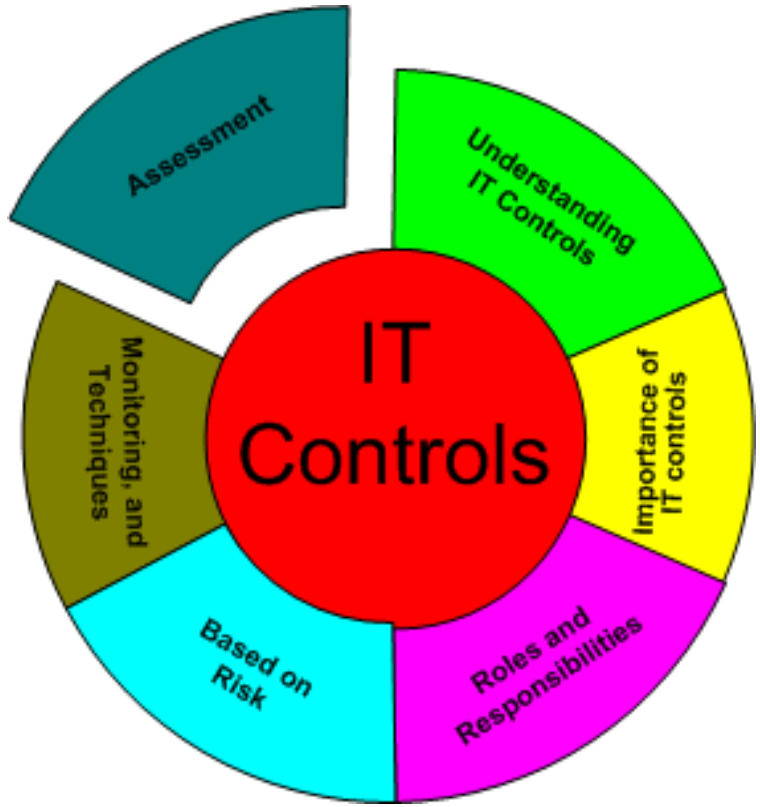
Monitoring & Techniques

- Monitoring & Assessing IT Controls
  - Choose a control framework
  - Use proper audit methodology
  - Ongoing monitoring/special review/automated continuous auditing



Assessment

- Assessing IT controls is an ongoing process, because business processes are constantly changing
- Technology continues to advance
- Threats evolve as new vulnerabilities emerge
- Audit methods keep improving



Change and Patch Management Controls

Why

- Why IT change and patch management controls are foundational to a healthy IT environment
- How IT change and patch management controls help manage IT risks and costs
- What works and doesn’t work in practice
- Describes sources of change and the likely impact on business objectives

Effective Change Management and Ineffective Change Management

- Compares effective change management (best practices) and ineffective change management (red flag indicators)
- Provides assessment tool and describes what internal auditors should do

The Top Five Steps To Reduce IT Change Risks

- The five prescriptive steps that can be taken immediately by most organizations to improve their change management processes are:
  1. Create tone at the top motivating the need for a culture of change management across the enterprise.
  2. Continually monitor the number of unplanned outages, which is an excellent indicator of unauthorized change and failures in change control.
  3. Reduce the number of risky changes by specifying well-defined and enforced change freeze and maintenance windows.
  4. Use change success rate as a key IT management performance indicator.
  5. Use unplanned work as an indicator of effectiveness of IT management processes and controls.

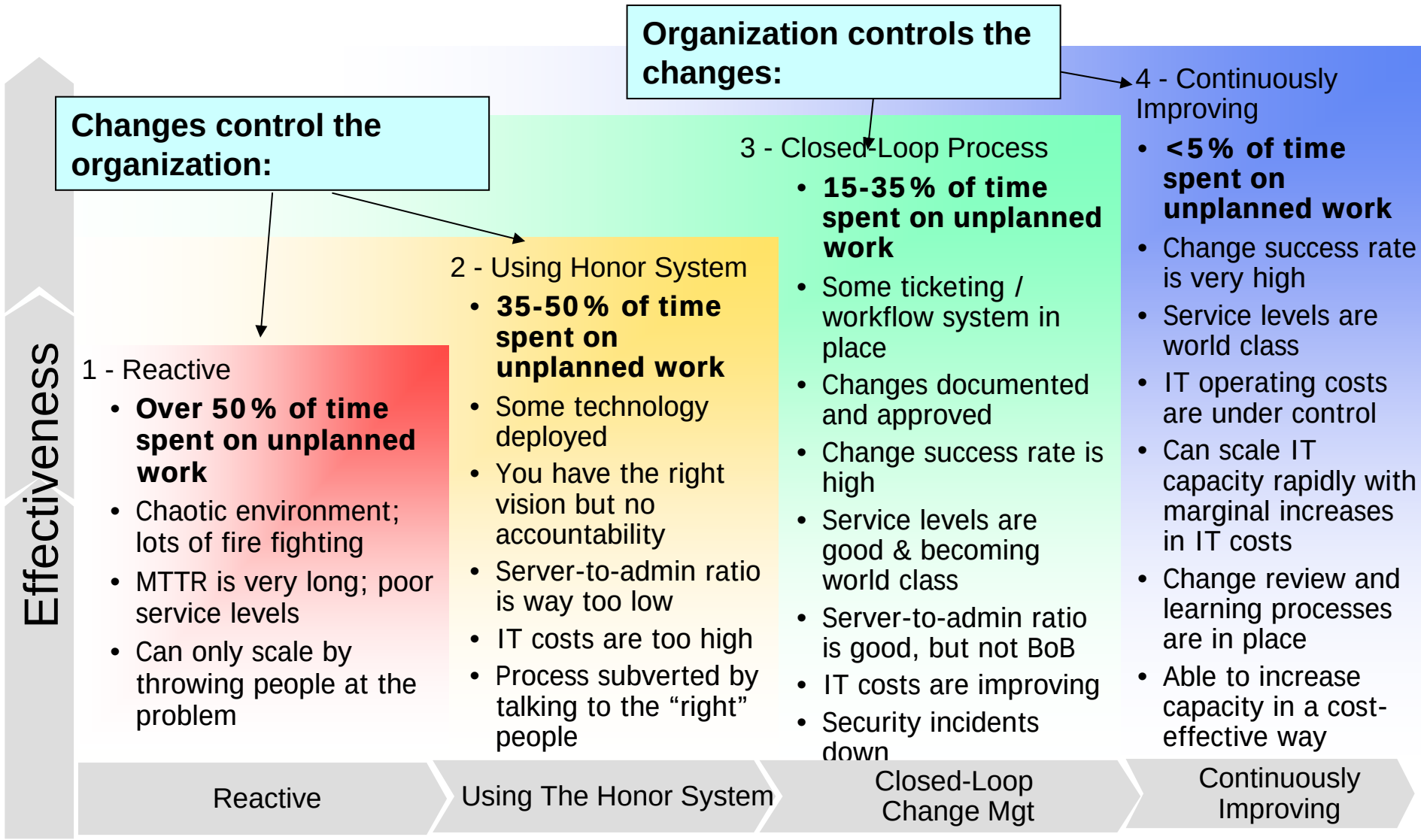
Understanding IT Change Management

- Business requirements drive the need for a high degree of IT uptime (availability) while regulatory requirements such as Sarbanes-Oxley drive the need for controls to ensure the confidentiality and integrity of information
- Stable and managed IT production environments require that changes be implemented in a predictable and repeatable manner
- IT personnel implementing changes must follow a controlled process that is defined, monitored and enforced
- Preventive controls (segregation of duties) and detective controls (supervisory) are needed in combination

Change and Patch Management

- Change and patch management is defined here as the set of processes executed within the organization's IT organization designed to manage the enhancements, updates, incremental fixes and patches to production systems, which include:
  - Application code revisions
  - System upgrades (applications, operating systems, databases)
  - Infrastructure changes (servers, cabling, routers, firewalls, etc.)

Change Management Maturity



Reactive

- The first level is Reactive. In this stage, IT groups typically spend most of their time firefighting and have problems with poor service levels and long outage times.
- There is usually very little formal process in place, and almost no systematic communication about changes that will be happening in the environment.
- Problems are usually discovered when there is an outage, or a user reports a significant problem to IT.
- Once a problem is reported, diagnosis is time-consuming because it’s difficult to tell where the problems are. There is little time to do proactive maintenance or documentation of systems and processes.

The Honor System

- As they begin to become dissatisfied with the thrash of life in the Reactive mode, companies generally move to *"Using The Honor System."*
- At this time, they may begin to document some policies and practices, and start to put some technologies in place to try to get a handle on uncontrolled changes in their infrastructure.
- Often, because there are really no "teeth" in the policies, there is frustration because nobody seems to be following them, and the tools are used inconsistently across the IT team.
- When problems happen, there is a lot of finger pointing and "not me" going on.
- Things improve over Reactive mode, but there is still a long way to go.

Using Closed-Loop Change Management

- Many organizations move to implementing closed-loop change management next.
- At this stage, there is typically a formal project (or at least strong exec sponsorship) to fix problems with change management and get service levels and IT costs under control.
- Companies often invest in trouble ticketing / workflow products at this point and implement more formal processes around change control in the organization.
- As capabilities become more mature at this level, the expectation develops that everyone will follow the formal change process, and there will be consequences for those who operate outside the process.
- There is generally a marked improvement in service levels and staff efficiency at this level of performance.

Continuously Improving

- Once they've tasted the success of Closed-Loop Management, companies begin to use their newly acquired control to pinpoint areas of problems and inefficiency.
- They are then able to systematically attack and improve weak areas, which allows continuous and ongoing improvement.
- Companies at this level, while not perfect, are able to provide predictable, high quality services in a cost-effective manner.

Why Audit Change Controls?

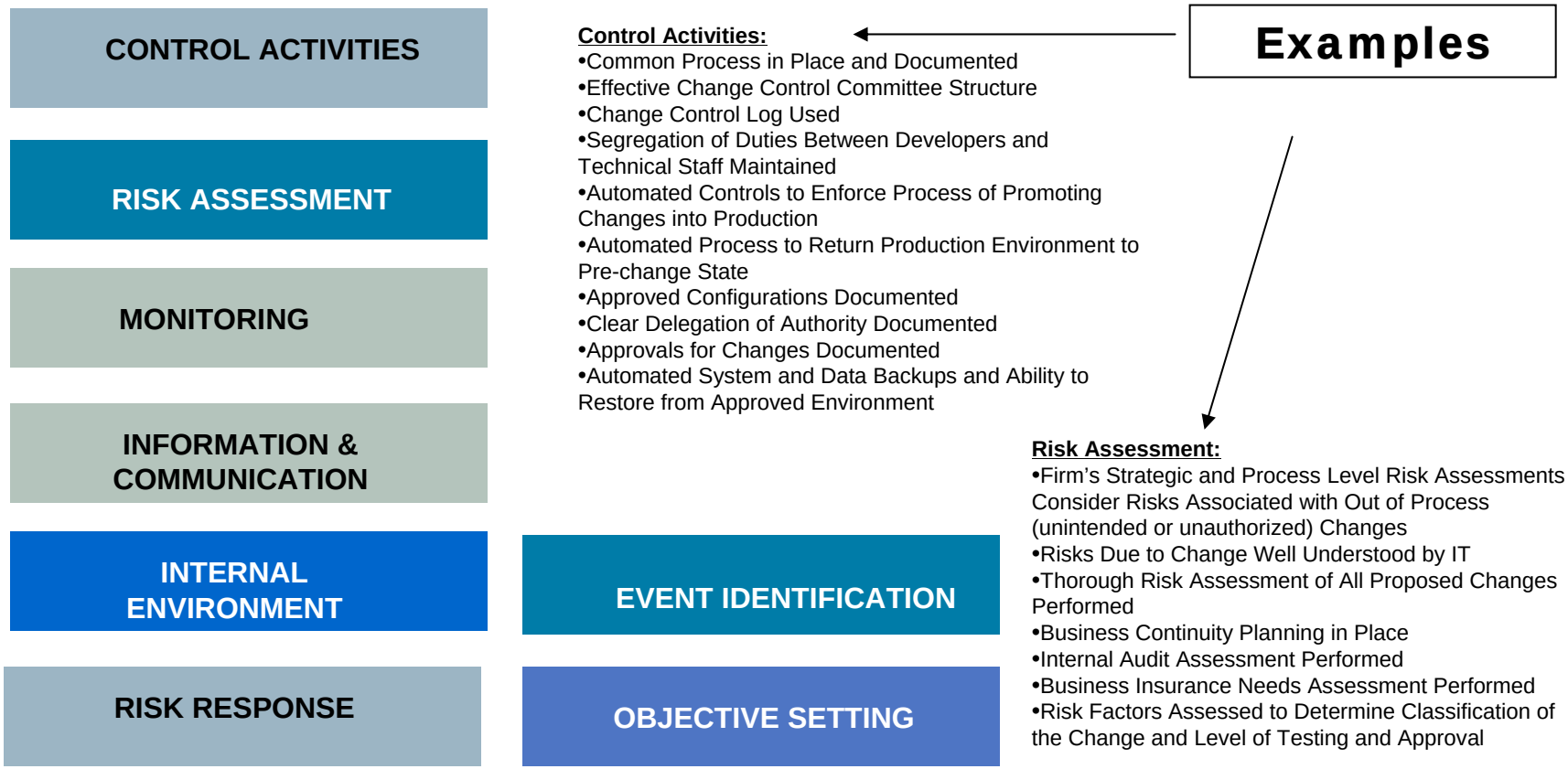
- Increased regulatory requirements around IT controls
  - Increased focus from Audit Committee and Senior Management
  - Internal auditors responsible for providing IT controls assurance
- Technology is everywhere
  - All business decisions result in at least one IT change. When changes are not controlled, they can impact the entire organization
  - According to analysts, 80% of all outages are due to change

Benefits of Good Change and Patch Management Processes

- Spend more time on new development work to advance business goals and objectives
- Reallocate IT staff resources to deliver new capabilities versus *“putting out fires”*
- Spend less time on unplanned IT work
- Less IT downtime
- Ability to install critical patches with minimal disruption

Assessing Change & Patch Management Processes

- COSO ERM Model For Change & Patch Management



Continuous Auditing

The Need for Continuous Auditing

- Today the need for continuous auditing is clear.
- Organizations are constantly exposed to significant errors, frauds, or inefficiencies that can lead to financial loss and increased levels of risk.
- The pressures of regulatory requirements and need to improve business operations are pushing organizations to ensure controls are working effectively and that risk is being properly mitigated.
- As a result, Internal Audit is turning to continuous auditing to help fulfill this expanded mandate.

Role of Continuous Auditing

- Today's audit challenges
  - Regulatory compliance & controls
  - Internal audit value and independence
  - Availability of skilled resources
  - Determining appropriate technology solutions
- Need for timely, ongoing assurance over risk management and control systems
- Role of continuous auditing
  - Provides more frequent, more timely, analyses to better manage control deficiencies and risk

The Focus of Continuous Auditing

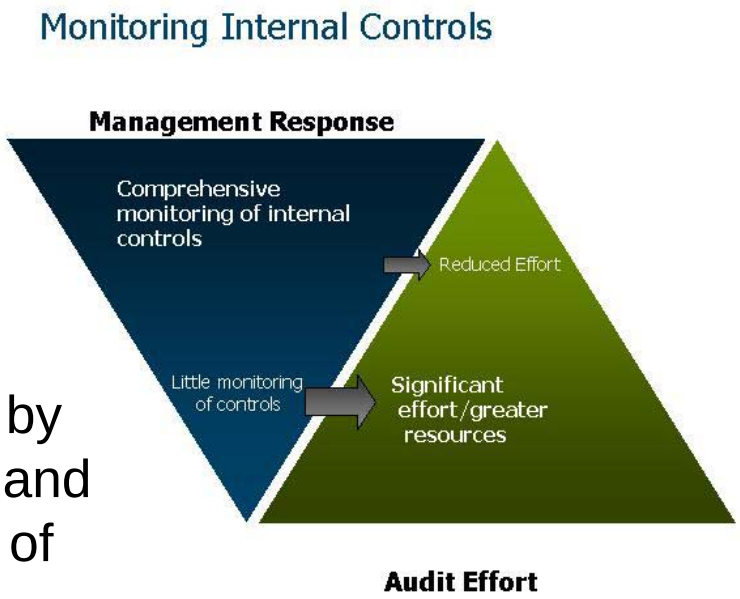
- One thing is certain. There is a great need for timely and ongoing assurance over risk management and control systems.
- The focus of continuous auditing is not simply on compliance with controls and regulations, but the improved efficiency of operations in the organization.
- Continuous auditing also should contribute to the overall improvement of the organization by identifying and assessing risk and providing information to management in order to better respond to changing business conditions.

The Definitions

- **Continuous Auditing**
  - Method used to perform audit-related activities on a continuous basis – includes control and risk assessment
  - Performed by Internal Audit
- **Continuous Monitoring**
  - Processes to ensure policies/processes are operating effectively and to assess adequacy/effectiveness of controls
  - Performed by operational/financial management; audit independently evaluates adequacy of management activities

Relationship of Continuous Auditing/Monitoring/Assurance

- Role of continuous auditing dependent on management's role in continuous monitoring of controls
  - Inverse relationship: the greater the role of management, the less of a direct role of internal audit



- **Continuous assurance**
  - Depends on effective monitoring by management of internal controls and Audit's independent assessment of that function

Application Areas

- **Continuous control assessment**
  - Identification of control deficiencies
  - Identification of fraud, waste, abuse
- **Continuous risk assessment**
  - Examination of consistency of processes
  - Development of enterprise audit plan
  - Support to individual audits
  - Follow-up on audit recommendations

Key Steps to Implementation

- Establish audit objectives and requirements
- Gain executive-level support
- Ascertain degree to which management is performing monitoring role
- Select appropriate technology solutions
- Identify information sources and gain access
- Understand business processes and identify key controls and risks
- Build audit skill set
- Manage and report results

Benefits

- Increased scope of audit activities
- Increased ability to mitigate risk
- Reduced cost of internal control assessment
- Increased confidence in financial results
- Improvements to financial operations
- Reduced financial errors and potential for fraud
- Reduced revenue leakage for improved bottom-line results
- Sustainable and cost-effective means to support compliance

Management of IT Auditing

The Changing Nature of Audit Function

- Information technology is changing the nature of the audit function.
- In this section the strategic issues involved during the planning, performance, and reporting of IT audits are discussed.

New Risks

- As new risks emerge, new audit procedures are required to manage these risks adequately.

Defining the IT Boundaries

- One of the initial challenges when developing the IT audit plan is defining the IT boundaries.
- The reality is that IT means different things to different organizations. Even two companies in the same industry may have radically different IT environments.
- Recognizing that there is a high amount of heterogeneity in IT environments, one way a one can approach the definition of IT is by thinking about it in layers.

The Key Layers to Consider are:

- **IT governance/management,**
- **Technical infrastructure,**
- **Applications and External connections.**

- Obviously, each organization is different, but this categorization should cover the majority of critical systems for most organizations.

Defining IT

Layer 1 - IT Governance/IT Management

- This layer comprises the set of people, policies, procedures and processes that govern/manage the IT environment.
  - IT Governance
  - Planning
  - System Monitoring
  - Software Development
  - Management of Outsourced Vendors

Defining IT

Layer 2 - Technical Infrastructure

- This layer refers to the systems that underlie, support, and enable the primary business applications.
  - Operating Systems
  - Databases
  - Networks

Defining IT

Layer 3 - Applications

- They are programs that perform specific tasks related to business operations.
  - **Transactional applications:** processes and records business transactions
  - **Supporting applications:** facilitate business activities but generally do not process transactions

Layer 4 - External Connections

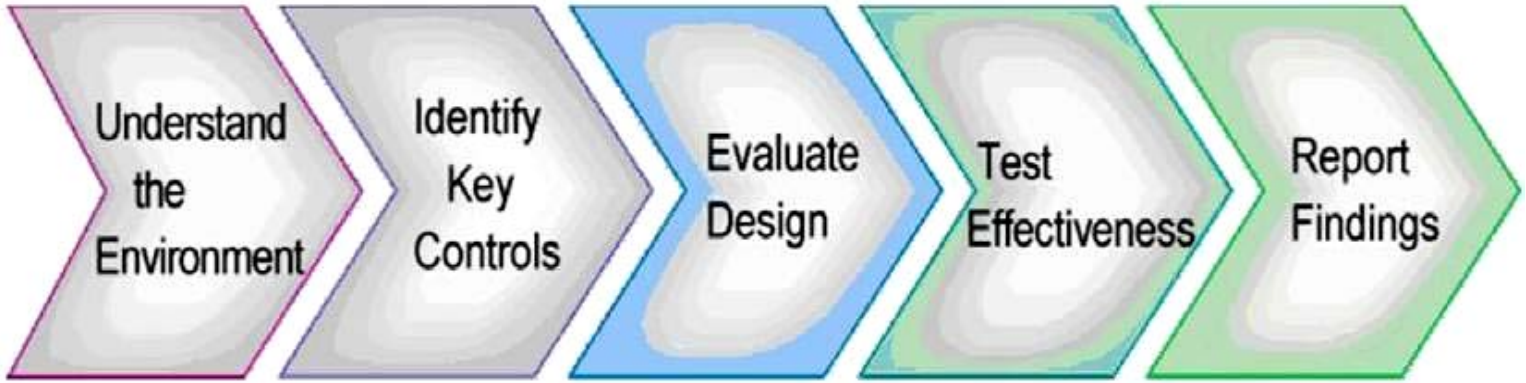
- Internet and other external networks

Defining IT Audit Universe

- Use overly broad definitions for IT audits
- Touch on all the layers in the IT environment
- IT audit resources are typically scarce, and IT audit demands are substantial.
- Understand how to build an IT audit plan that effectively balances IT audit needs with resource constraints.

Executing IT Auditing

- Normal Audit process



- Consider IT audit by using frameworks and standards, such as
  - COSO, CoBIT, ISO 27001…

Managing IT Auditing

- Require new management techniques and procedures
- Manage IT Audit Resource
  - Identify, hire, train and retain competent IT audit professionals
  - Consider certifications, rotation, continuing education
  - Co-source IT audit function

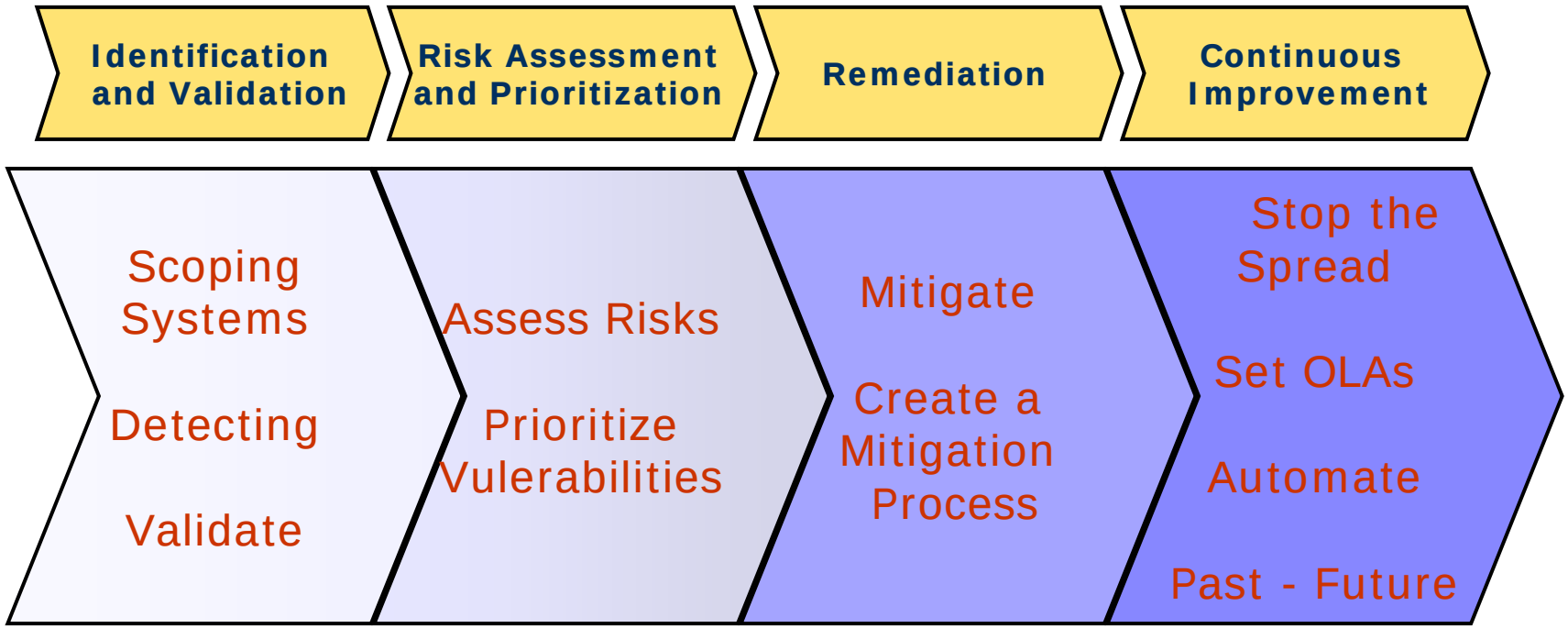
Managing IT Auditing

IT Audit Accelerators

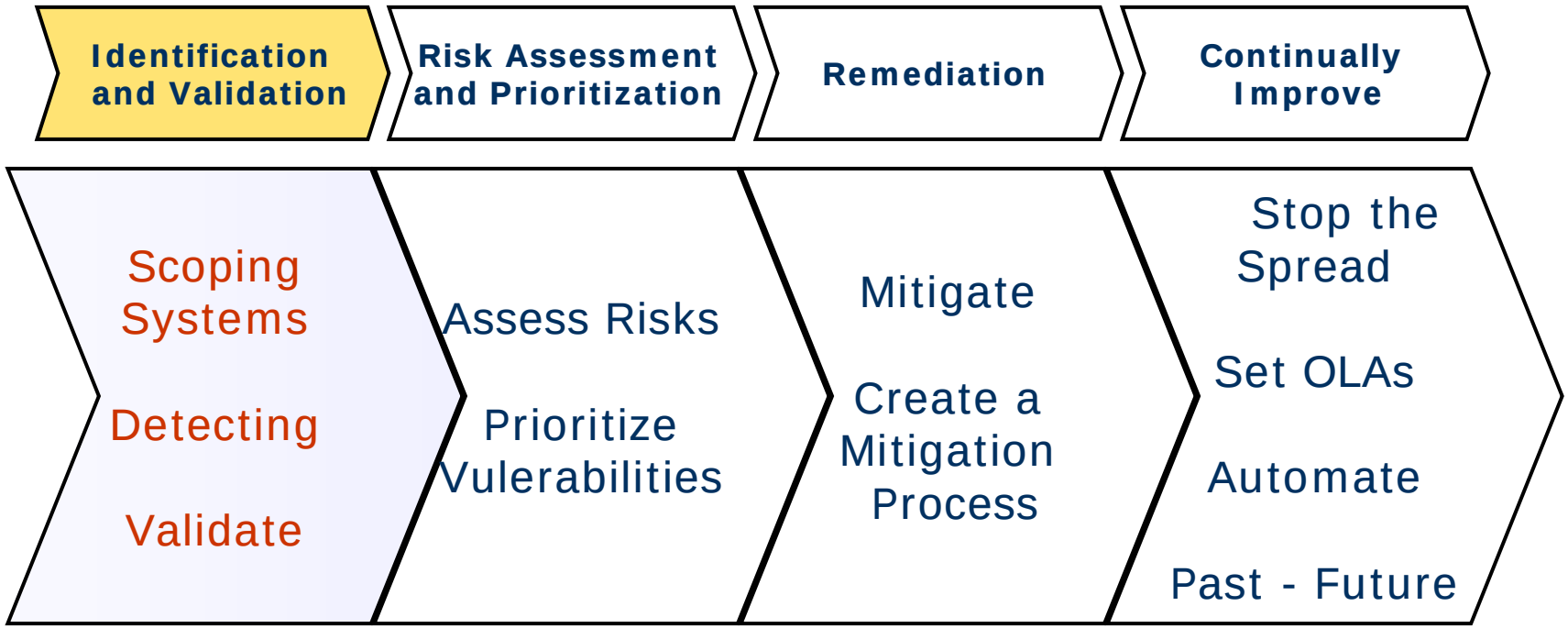
- Audit facilitators, such as
  - Electronic work papers
  - Project management software
  - Flowcharting software
- Testing Accelerators, such as
  - Data analysis software
  - Security analysis tools

Managing and Auditing IT Vulnerabilities

Vulnerability Management Lifecycle



Vulnerability Management Lifecycle



Scoping Systems

- Acquire a complete list of all network segments used throughout the organization, including
  - corporate wired and wireless networks,
  - production networks,
  - backup or administration networks,
  - transit networks,
  - laboratories and testing networks,
  - remote offices, and
  - so on.
- Network diagrams.

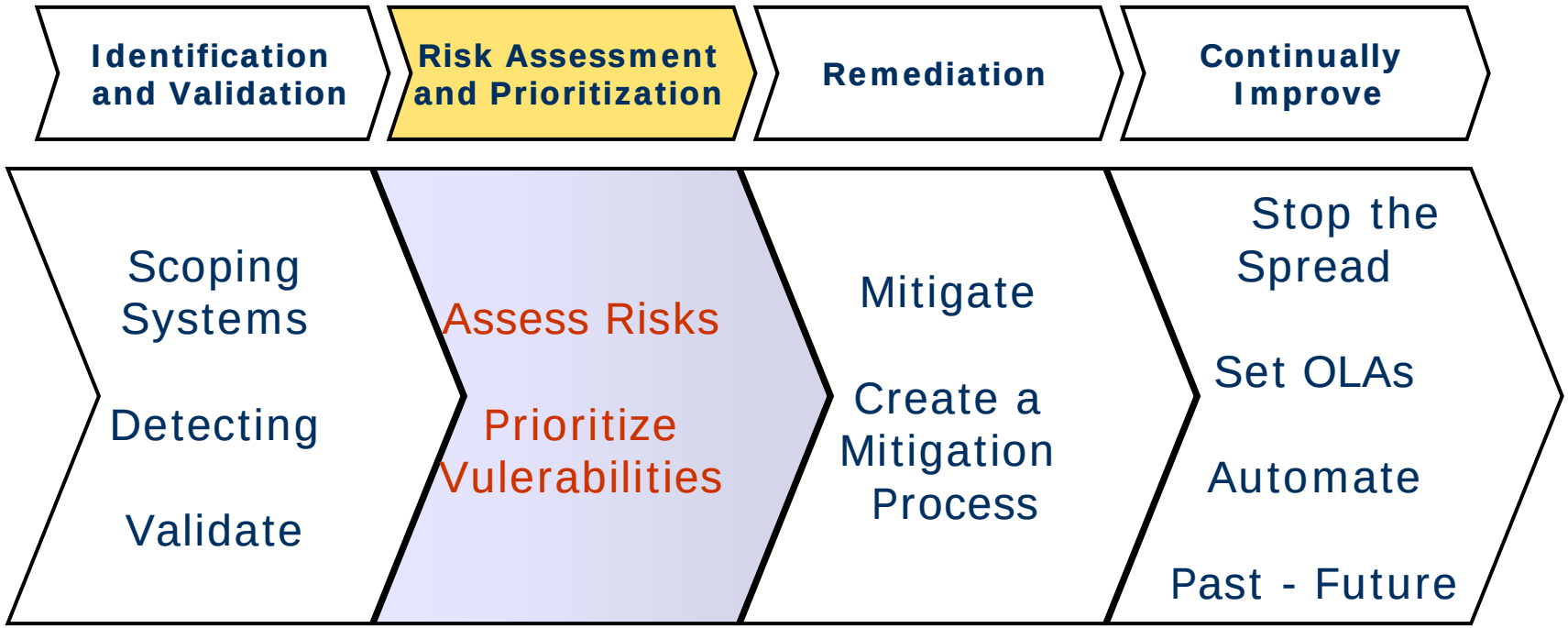
Detecting Vulnerabilities

- Daily, monthly or quarterly - **all IT assets** connected to each network segment should be scanned or monitored periodically for vulnerabilities.
  - These assets include devices such as
    - business application servers (database, e-mail, Web, customer relationship management servers, and etc.),
    - security devices,
    - telecommunication and networking devices, and
    - printers.
- Monitoring refers to **software agents** installed on IT assets that report host configuration information.
- It also refers to network devices that continuously listen to network traffic and report (optionally block) malicious traffic that may exploit a vulnerability.
- These devices also are useful for identifying rogue or previously unknown IT assets.
- They are considered a preventive security control, because of their ability to block attacks before they cause loss.

Validating Findings

- The sophistication and accuracy of vulnerability scanning and monitoring devices are generally quite good.
- However, they always have limitations.
- Errors can occur in the form of false positives or false negatives.
- A **false positive** is a vulnerability that has been reported, but does not exist, because the detection mechanism was in error.
- A **false negative** occurs when a vulnerability exists, but the detection system failed to identify it.

Vulnerability Management Lifecycle



Assessing Risks

- Organizations must have a well-defined procedure for measuring risk that can be applied quickly and accurately.
- The presence of a vulnerability does not always warrant remediation, and the organization may choose to accept the risk posed by the vulnerability.
  - For example, when existing security controls sufficiently reduce the likelihood of a successful attack, or when the asset targeted is of little or no value.
- In these cases, the risk acceptance should be documented and approved to avoid later having to reassess the same finding.

Prioritizing Vulnerabilities

- From there you prioritize remediation according to the criticality of the vulnerable asset, the likelihood or frequency that an attack will occur and the effort required to implement the fix.
- The organization also may want to examine the causes of past security incidents and prioritize accordingly.
  - For example, perhaps past incidents were due to breaches initiated from third-party connections or perhaps they were caused by malicious software introduced by employees.

Risk Rating

• If a risk falls in one of the boxes numbered **15 – 25**, immediate action required, so far as is reasonably practicable
• If a risk falls in one of the boxes numbered **8 – 14,** prompt action required, so far as is reasonably practicable
• If a risk falls in one of the boxes numbered **4** – 7, risk reduction required, so far as is reasonably practicable
• If a risk falls in one of the boxes numbered **1 – 3**, further risk reduction may not be feasible or cost effective

EXAMPLE

Risk Matrix

Likelihood	Consequence				
	1 Insignificant	2 Minor	3 Moderate	4 Major	5 Catastrophic
1 - Rare	1	2	3	4	5
2 – Unlikely	2	4	6	8	10
3 – Possible	3	6	9	12	15
4 – Likely	4	8	12	16	20
5 – Almost Certain	5	10	15	20	25

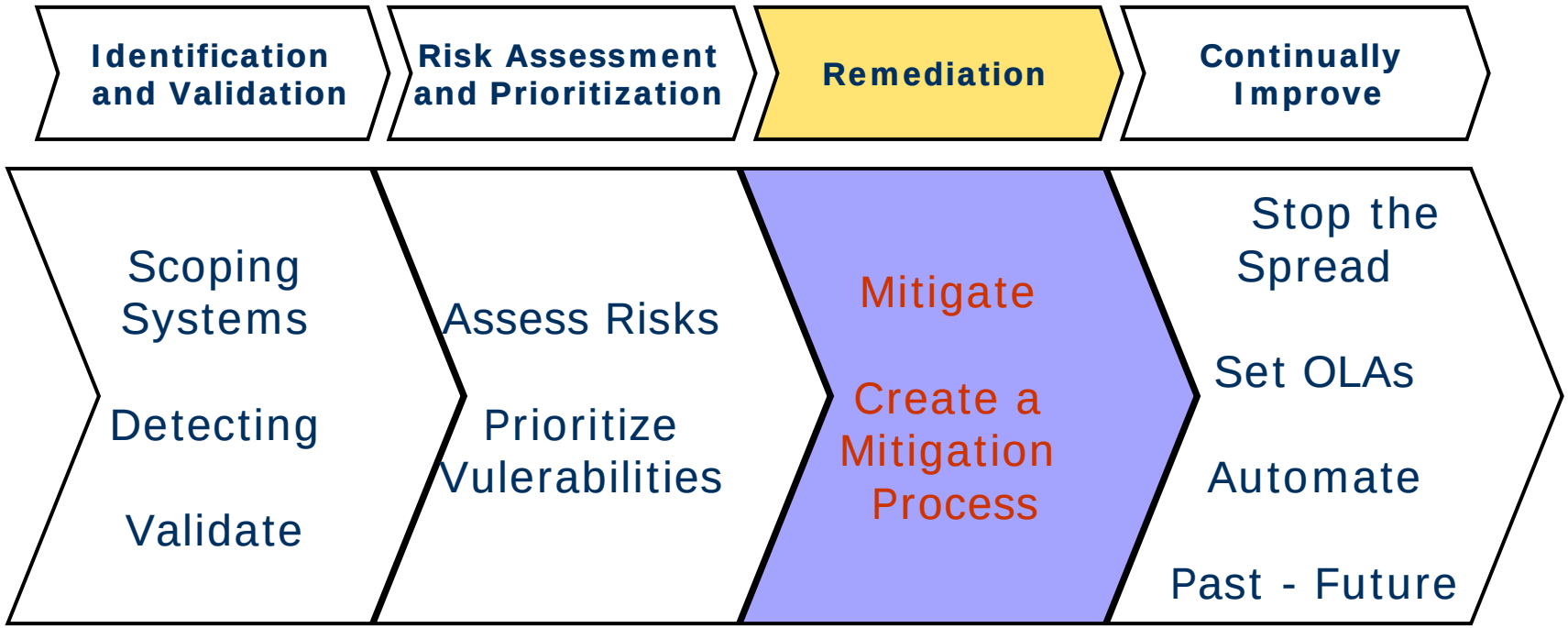
EXAMPLE

Frequency (assessment of likelihood of occurrence)

1	Rare	Only occurs in exceptional circumstances, <1%, 1 – 5 year strategic risk
2	Unlikely	Could occur at some time, 1 – 5%, at least annually
3	Possible	Should occur at some time, 6 – 20%, at least monthly
4	Likely	Will probably occur, 21 – 50%, at least weekly
5	Almost Certain	Expected to occur, > 50%, at least daily

EXAMPLE

Vulnerability Management Lifecycle



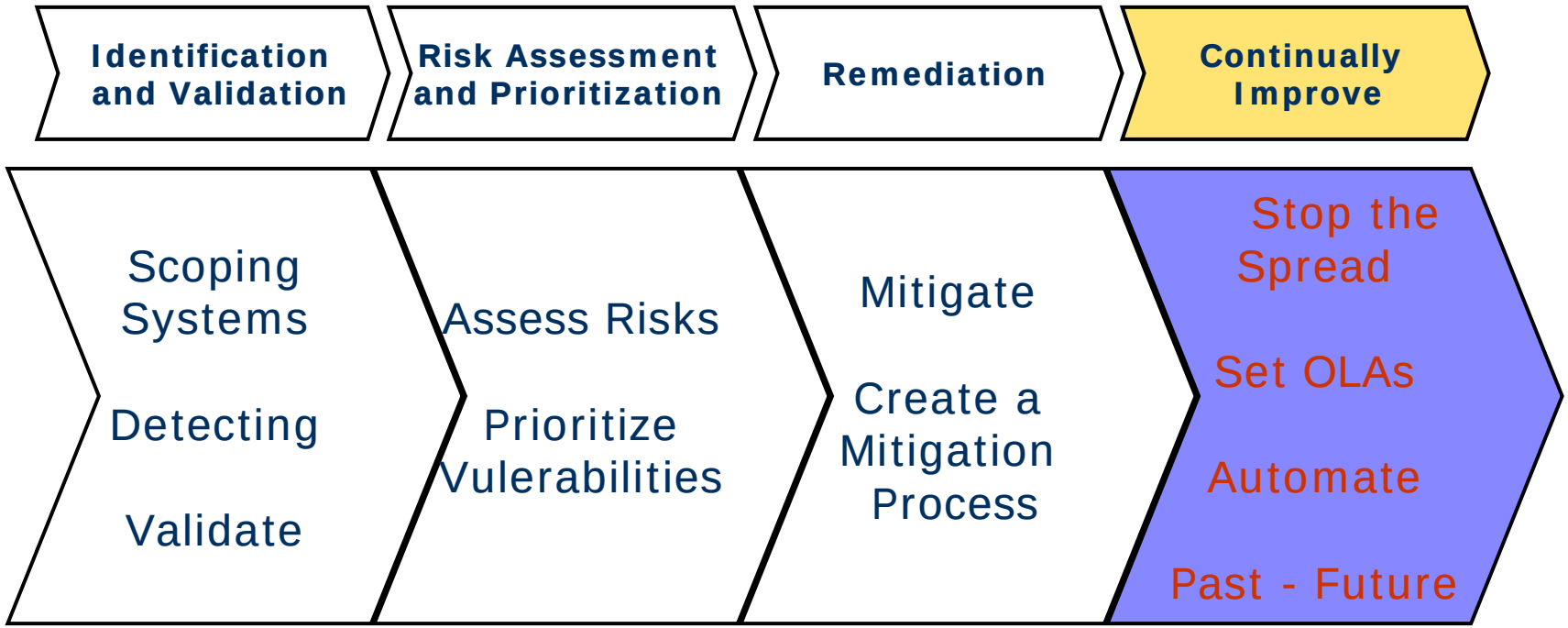
Mitigating Critical Vulnerabilities

- Often the best way to fix the most critical vulnerabilities is for IT security staff to use the existing incident or trouble ticketing system.
- This system is probably part of a standard IT operating procedure, which ensures fixes are addressed in a timely manner by the appropriate personnel.
- Critical vulnerabilities are handled by Incident Management which coordinates remediation efforts with Change Management using emergency change procedures that expedite the implementation into production.
- Non-critical vulnerabilities are reviewed via the standard Change Management process.
- Once approved, Release Management then prepares, tests and facilitates the change.
- Again, Change Management reviews the change to ensure it met all requirements and finally the Configuration Management database is updated to reflect these improved (i.e. more secure) modifications.
- Note that regardless of whether the remediation work is an emergency or not, all changes are routed through Change Management. They act in a marshalling role to move the change through the IT machinery to a successful completion.

Creating a Vulnerability Mitigation Process

- Fixing the most critical vulnerabilities removes obvious dangers.
- This is should be a quick process to execute, because there may be a couple of vulnerabilities.
- However, different challenges arise when trying to remediate hundreds or thousands of vulnerabilities at a time.
- The most efficient way to execute these fixes is to create an IT project that includes a project manager, process deliverables, and deadlines.
- The project must then have the authority to integrate with the organization's Change Management process to deploy the necessary patches.
- Implementing a well-designed vulnerability management project with a Change Management process is the best way to achieve repeatable and effective vulnerability management.

Vulnerability Management Lifecycle



Stop the Spread

- Inputs into configuration management.
- With vulnerabilities being addressed through standard IT business processes, IT security should communicate any permanent system or application modifications with Change Management to ensure future builds are released with more secure configurations.
- This notification is critical and one of the few proactive steps involved in vulnerability management.
- To ensure this communication takes place, the security organization should have a direct relationship with Change Management and/or whichever groups manage desktop, server, and application builds.

Achieve Efficiency Through Automation

- The efficiency of a vulnerability management group is vastly improved through automation.
- The more the organization can automate processes, such as
  - scanning for vulnerabilities,
  - creating tickets with operational groups,
  - status updates, and
  - reporting

the more it will be able to focus on further improving and scaling its efforts — or, indeed, spending fewer resources on IT security.

- Whoever is responsible for actually deploying the patches should use automated patching solutions, as it is rarely cost effective to apply them manually.

Use Past Experience to Guide Future Actions

- Organizations can use past problem indicators
  - such as patch failure rate/change success rate — to rate the risk of changes.
    - For example, if a specific type of change has been historically problematic, the risk of deploying future patches of that type can be decreased by increasing pre-deployment testing practices.

Audit Scope

Identification and Validation Asset Inventory Detect Vulnerabilities Validate Findings	**Remediation** Monitoring Incident Management Change Management Patch Testing
Risk Assessment and Prioritization Risk Assessment Vulnerability Priorities	**Maintenance and Improvement** Configuration Management Operation-Level Agreements Policies and Requirements

Organizational Maturity

Identification and Validation

Low Performer

- Small % of IT assets are scanned and managed – or cannot measure what is being managed.
- Incomplete or limited network architecture diagrams.
- Inability to validate scanning results.
- Limited remediation or no remediation.
- No asset management system.
- High level of configuration variance

High Performer

- Effective asset management
- Know % of critical assets scanned and managed.
- Scans are validated and false positives are identified.

Organizational Maturity

Risk Assessment and Prioritization

Low Performer

- Unable to distinguish between critical and non-critical IT assets and prioritize.
- Excessive number of vulnerabilities to be fixed.

High Performer

- Ongoing IT risk assessment.
- Cost of remediation is evaluated.
- Utilizes prior patch and change metrics to determine high risk patches.

Organizational Maturity

Remediation

Low Performer

- Patch management is not automated.
- Lack of patch testing.
- More work than the IT organization can handle.
- No configuration management or is not integrated with vulnerability management.
- Unplanned work.

High Performer

- System configures are standardized.
- Organizational engagement.
- Automated patching which includes patch testing.
- Remediation is tracked and validated.

Organizational Maturity

Continually Improve

Low Performer

- Few automated processes.
- Nonexistent OLAs.
- Reactionary.
- Security incidents are detected when they cause disruptions.
- No record of patch or change success rate.

High Performer

- Inputs into configuration mgmt for secure builds.
- Increased scanning frequency and coverage.
- Devices are analyzed prior to production.
- Standard IT configs.
- Patching risks are identified.

Key Metrics

- Percent of total systems monitored or scanned.
- Number of unique vulnerabilities.
- Percent of systems managed.
- Percent of validated vulnerabilities.
- Mean time to remediate.
- Operational Level Agreement (OLA)s
- Time spent on unplanned work.
- Number of security incidents.
- Impact of security incidents.

IT Outsourcing

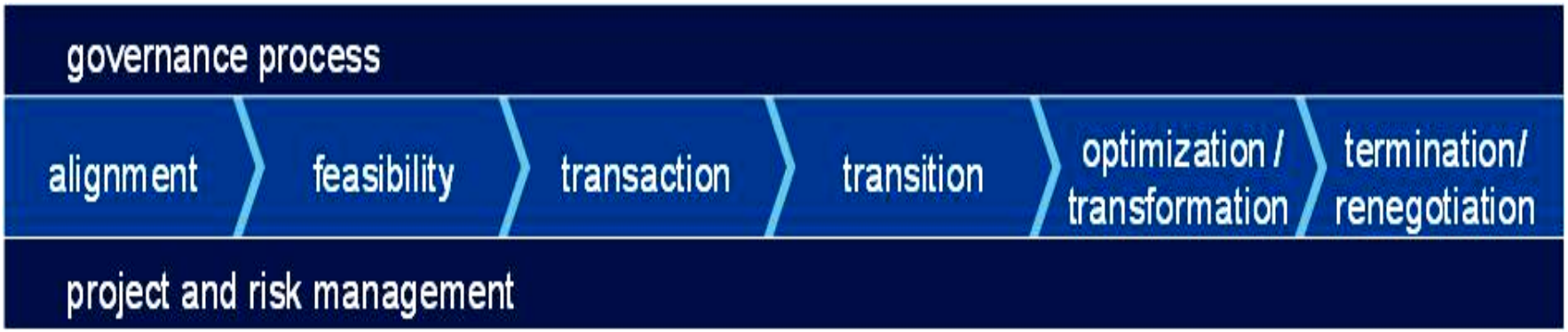
Information Technology Outsourcing

- Information technology outsourcing has grown in popularity as an efficient, cost-effective, and expert solution designed to meet the demands of systems implementation, maintenance, security, and operations.
- The benefits of IT outsourcing are accompanied with the need to manage the complexities, risks, and challenges that come with it.
- It is management's role to decide whether, where and what to outsource.
- But it is important that auditors understand the outsourcing context and help the organizations with a comprehensive review of its outsourcing operations and evaluation of its compliance with applicable laws and regulations

Major Types of IT Outsourcing

- Application management
- Infrastructure management.
- Help desk services.
- Independent testing and validation services.
- Data center management.
- Systems integration.
- R&D services.
- Managed security services.

Outsourcing Life Cycle



- Each successful initiative begins with a careful consideration of the business case, which specifies the investment schedule and the expected business benefits in terms of cost reduction and maximized work efficiency over a three- to five-year period.
- A well-constructed business case also indicates how identified benefits are to be accomplished through a careful alignment of vendor selection, an established transition and process improvement approach, and the use of risk and security solutions.

IT Outsourcing Risks (1)

Here is some examples of risks related IT Outsourcing.

Strategy: Outsourcing strategy is not aligned with corporate objectives.
Feasibility: Assumptions (e.g., payback period, customer and supply-chain impacts, and cost savings) are wrong as the result of inadequate due diligence from suppliers and the organization's failure to assess relevant risks.
Transaction: Procurement policies are not met; proper service-level agreements are not implemented; operational, human resources (HR), and regulatory implications are not considered; and contingency arrangements are not planned.

The Impact of Those Risks (1) Could Be:

- The contract is not set up and managed in line with corporate objectives.
- The potential for outsourcing is not explored in detail, resulting in the lack of fully derived benefits. The contract is awarded to an inappropriate supplier.
- Supplier issues are not managed efficiently and effectively because they were not anticipated properly.
- Absence of a well-drafted agreement could lead to a situation in which the client might be unable to fall back on a legally binding document to ensure compliance by the vendor to intended contractual terms.
- Potential breaches of regulatory compliance exist that lead to financial penalties and negative repercussions on the company's brand.

IT Outsourcing Risks (2)

Some more examples

Transition: There is a lack of formal transition planning, failure to plan for retention of appropriate skills, and an ineffective escalation and resolution of operational IT issues.
Optimization and Transformation: The outsourcing contract is not managed effectively. Therefore, outsourcing benefits and efficiencies are not achieved.
Termination and Renegotiation: There is an inadequate termination of outsourcing processes.

The Impact of Those Risks (2) Could Be:

- There is a loss of key resources during the transition period.
- There is a loss of customer confidence in the outsourced service.
- The return on investment is not what was expected or is minimal compared to the outsourcing costs.
- The organization provides services that fall below established expectation levels.
- There is a rise in unplanned costs.
- The company is unable to take over the outsourced activity at a later date or is unable to terminate or renegotiate the contract.

Key Control Considerations – Client Operations

Governance Outsourcing Framework

- Align every IT outsourcing contract with the organization's key business objectives
- Set up a monitoring mechanism
- Manage changes in IT projects and services across complex portfolios.
- Establish direct and visible accountability for IT performance.
- Define specific ownership of key contract terms.
- Define well-integrated IT management processes for the client and service provider.

As an Auditor, Key Questions You Should Ask Include:

- How transparent is the governance process?
- Do formal relationship management processes address outsourcing conflicts and build effective working relationships between contracting parties?
- Are roles, responsibilities, and delegation of authority activities defined clearly between contracting parties?
- Are communication channels established clearly?

Key Control Considerations – Client Operations

Alignment

- Validating the strategy.
- Identifying options.
- Preparing the business model.
- Agreeing on sponsorship and building the team.

Feasibility

- Building the business model and case.
- Creating the baseline.
- Understanding the market.
- Assessing and benchmarking options.

The Alignment and Feasibility Phase

- The alignment and feasibility phase deals with the formalization of the IT outsourcing strategy.
- During this phase, the client should prepare a business case that is based on various IT outsourcing models and an assessment of outsourcing options that is based on research and benchmarking.
- The outsourcing strategy chosen needs to detail the portfolio of services that will be assigned to one service provider or to multiple service providers and the location of these services (i.e., onsite or offsite).
- The different outsourcing models usually include build-operate-transfer activities, joint ventures with service providers, or a combination of both.

Key Audit Considerations Include:

- Is the client’s IT outsourcing strategy aligned with the company's overall business strategy?
- Did the client consider properly all financial, operational, and legal considerations before embarking on the IT outsourcing partnership?
- Are outsourcing assumptions validated by research or data?

Key Control Considerations – Client Operations

Transaction

- Structuring the deal.
- Agreeing on outsourced assets.
- Negotiating the contract.
- Delivering the deal and the business case.

The Transaction Phase

- The transaction phase covers selecting vendor, structuring the deal, negotiating the contract and delivering the deal and business case;
- Vendor selection requires a comprehensive evaluation of the service provider's technical competencies and constraints and is based on the organization's outsourcing service needs.
- Although there is no right or wrong approach, organizations should follow the steps, such as plan, preparation, gathering vendor’s data, conduct due diligence, negotiation the contract and close the deal.

Key Audit Considerations Include:

- Determining whether the vendor selection process was conducted in a fair manner.
- Examining the contract's description of aspects the client will be exposed to once the outsourcing partnership begins.
- Identifying whether a checklist exists that consists of the legal and contractual factors agreed on by the client and service provider and that help to determine the vendor's compliance with each of these factors.

Key Control Considerations – Client Operations

Outsourcing Contract Key Components

- **Service levels and incentives**
  - Vendor personnel
  - Data protection, privacy, and intellectual property
  - Price protections
  - Third-party assignments
  - Ownership of assets used or created by partnership
  - Conflicts among different legal systems
  - Contingency planning and change management
  - Notice of adverse material impacts
  - Right to audit
  - Termination

Key Control Considerations – Client Operations

Transition

- Delivering the change.
- Getting quick returns on investment.
- Establishing the culture.
- Managing people.

Change Management

Optimization & Transformation

- Monitoring the contract and resolving disputes.
- Transforming the business.
- Reassessing the relationship.
- Delivering the business case – realizing the benefits.

Transitioning

- Transitioning or migration involves the transfer and ownership of knowledge to an entity with no previous experience with a given system, process, corporate culture, or industry.
- During this stage, the client and service provider could experience high levels of change.
- Both client and service provider should show necessary change management experience to deal with any disruptions caused by the transition process;
- Transformation and Optimization includes monitoring contracts, resolving disputes, reassessing the relationship and realizing business benefits.

Key Control Considerations – Service Provider Operations

- **Control environment**
- **Security considerations**
  - Data protection risks
  - Security - network, physical, environment, personal and logical access
  - Business continuity
- **SDLC controls**
- **Change management controls**
- **HR policies and procedures**

Service Provider Operations

- As part of the IT outsourcing venture, some of the client’s controls may be transferred to the service provider totally or in part.
- In such cases, the audit's scope extends beyond the client’s operations.

Evaluating the Service Provider's Control Environment

- The internal auditor plays a critical role in evaluating the service provider's control environment.
- As a result, auditors need to assess the strength of the control framework and control activities affecting the outsourced processes, as well as inform management on the effectiveness of outsourcing operations from a compliance and operations standpoint.
- To do so, auditors should evaluate and test the service provider's policies, procedures, guidelines, risk assessments, and SDLC control monitoring activities, as well as obtain independent information through the established communication channels.
- Auditors also can rely on the international standards adopted by the service provider for compliance, and evaluate the service provider's documentation to identify whether controls were customized to fit the client’s unique environment.

Top 10 Questions Auditor Should Ask

1. Are the services outsourced significant to the client?
2. Does the client have a well-defined outsourcing strategy?
3. What is the governance structure relating to outsourced operations? Are roles and responsibilities clearly defined?
4. Was a detailed risk analysis performed at the time of outsourcing, and is a regular risk analysis being done?
5. Do formal contracts or SLAs exist for the outsourced activities?

Top 10 Questions Auditor Should Ask

6. Does the SLA clearly define KPIs for monitoring vendor performance?
7. How is compliance with the contract or SLA monitored?
8. What is the mechanism used to address noncompliance with the SLA?
9. Are the responsibilities of the ownership of data, system, communication system, operating system, utility software, and application software clearly defined and agreed upon with the service provider?
10. What is the process of gaining assurance on the operating effectiveness of the internal controls at the service provider's end?

Auditing Application Controls

Application Controls

Objectives:

- Input data is accurate, complete, authorized, and correct
- Data is processed as intended in an acceptable time period
- Output and stored data is accurate and complete
- A record is maintained to track data processing from input to storage to output

Application Controls

- One of the most cost effective and efficient approaches that companies use to manage the risks associated with business processes associated with applications is through the use of **controls that are inherent or embedded** into transactional and support applications as well as controls that are configurable.

Application Controls

- There is a direct correlation between complexity of transactions and support applications and the availability, use, and reliance on inherent and configurable application controls.
- In other words, a less complex IT infrastructure may not offer as many inherent or configurable application controls for risk management.
- Hence, the degree of transactional and support application complexity will drive the scoping, implementation, level of effort and knowledge required to execute an application control review, as well as the degree to which internal auditors can assist in a consulting capacity.

Application Controls

- Cost effective and efficient means to manage risk
- Reliant on the effectiveness on the IT general control environment
- Approach varies for complex versus non-complex environments

Benefits of Application Controls

- Reliability
  - Reduces likelihood of errors due to manual intervention
- Benchmarking
  - Reliance on IT general controls can lead to concluding the application controls are effective year to year without re-testing
- Time and cost savings
  - Typically application controls take less time to test and only require testing once as long as the IT general controls are effective

Reliability

- Application controls are more reliable than manual controls when evaluating the potential for control errors due to human intervention.
- Once an application control is established, and there is little change to the application, database, or supporting technology, the organization can rely on the application control until a change occurs.

Benchmarking

- If IT general controls that are used to monitor program changes, access to programs, and computer operations are effective and continue to be tested on a regular basis, the auditor can conclude that the application control is effective without having to repeat the previous year's control test.
- This is especially true if the auditor verifies that the application control has not changed since the auditor last tested the application control.
- Benchmarking is particularly effective when companies use pre-packaged software that doesn't allow for any source code development or modification.
- In cases like these, the company needs to consider more than just the code change.
- An application control within a complex application, such as SAP or Oracle Financials, can be changed, disabled, or enabled easily without any code change.

Scoping the Review

- **Business Process Method**
  - Top down review
- **Single Application Method**
  - Focus on a single application or module
- **Access Controls**
  - Included no matter which method is chosen

Business Process Method

- The business process scoping method is a top-down review approach used to evaluate the application controls present in all the systems that support a particular business process.
- Over the last several years, this method has grown in importance as the most common and widely accepted scoping methodology.

Single Application Control

- The single application scoping method is used when the auditor wants to review the application controls within a single application or module as opposed to taking a business process scoping approach.

Access Controls

- No matter what method is chosen to scope the review of application controls, the module's or application's logical access controls need to be reviewed periodically.

Review Approaches

- Planning
- Need for specialized resources
- Documentation
- Testing
- Computer-assisted audit techniques (CAATs)

Planning

- During planning all of the required audit resources need to be included on the planning team.
- This is also the time when IT specialists need to be identified and included as part of the planning process.
- Discussions should be held to ensure that management concurs with all identified risks and controls.

Need for specialized resources

- Important to identify if specialized IT auditors or special tools are required to assess and report on the effectiveness of application controls.
  - An example of when specialized resources are required involves a segregation of duties' review during the installation of an Oracle eBusiness Suite application for a large manufacturing company.
  - The complexity of the roles and functions contained within the application and database require the use of personnel with knowledge on the configuration capabilities of the Oracle application.
  - Additional staff may be needed who know how to mine data from the Oracle application and database to facilitate the review.
  - Furthermore, the review team may need a specialist who is familiar with a specific computer-assisted audit tool to facilitate data extraction and analysis.

Common Application Controls

- **Input and access controls**
  - Data checks and validations
  - Automated authorization, approval, and override
- **File and data transmission controls**

Common Application Controls (Cont.)

- **Processing controls**
  - Automated file identification and validation
  - Automated functionality and calculations
  - Audit trails and overrides
  - Data extraction, filtering, and reporting
  - Automated functionality and aging
  - Duplicate checks
- **Output controls**
  - General ledger and sub-ledger posting
  - Update authorization

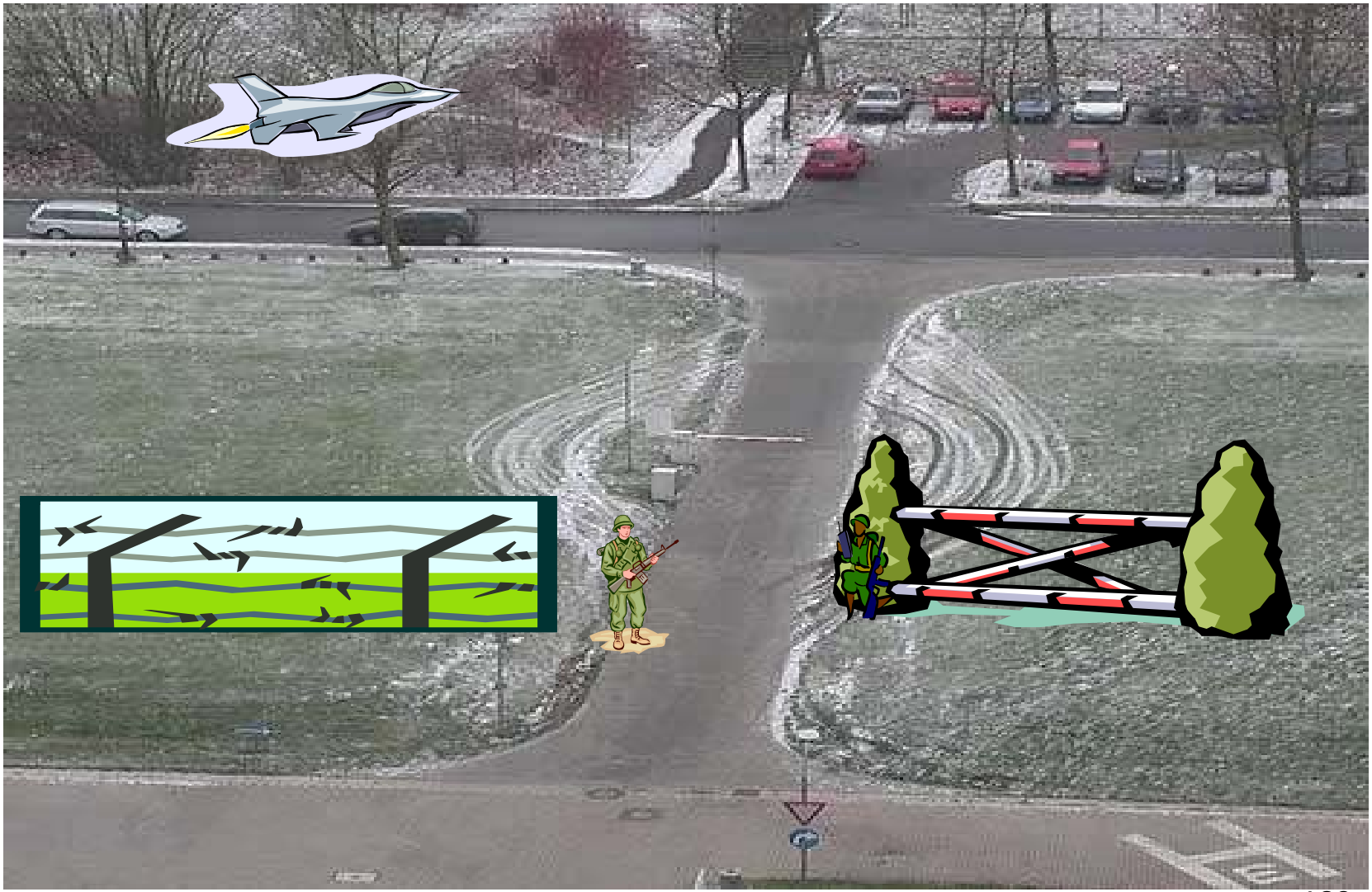
Sample Detailed Review Program

- **Suggested tests**
  - Test input controls to ensure transactions are added into and accepted by the application, processed only once and have no duplicated
  - Test processing controls to ensure transactions are accepted by the application, processed with valid logic, carried through all phases of processing and updated to the correct data files

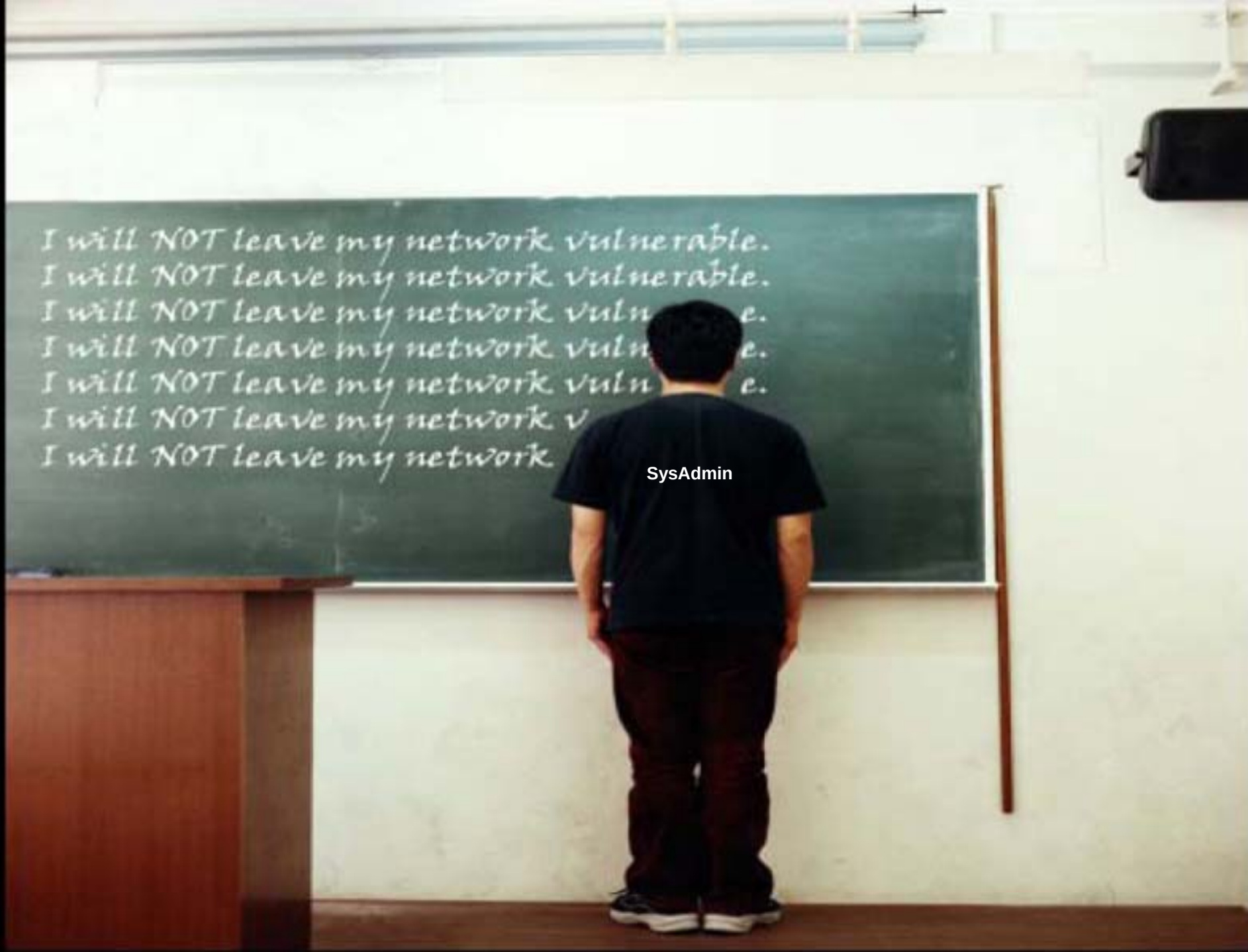
Very Short Summary

Secure Enough?

There is NO single IA "Silver Bullet"



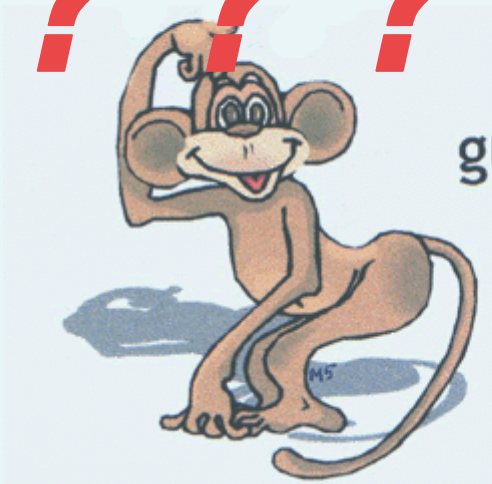

Bishopbriggs
Leisure Centre


I will NOT leave my network vulnerable.
I will NOT leave my network vulnerable.
I will NOT leave my network vuln e.
I will NOT leave my network vuln e.
I will NOT leave my network vuln e.
I will NOT leave my network v
I will NOT leave my network
SysAdmin

Gingsberg Theorem

- You can't win!
- You can't break even!
- You can't even quit the game!

Who came first ?
Audit or Information Security?



Questions
are
guaranteed in
life;
Answers
aren't.